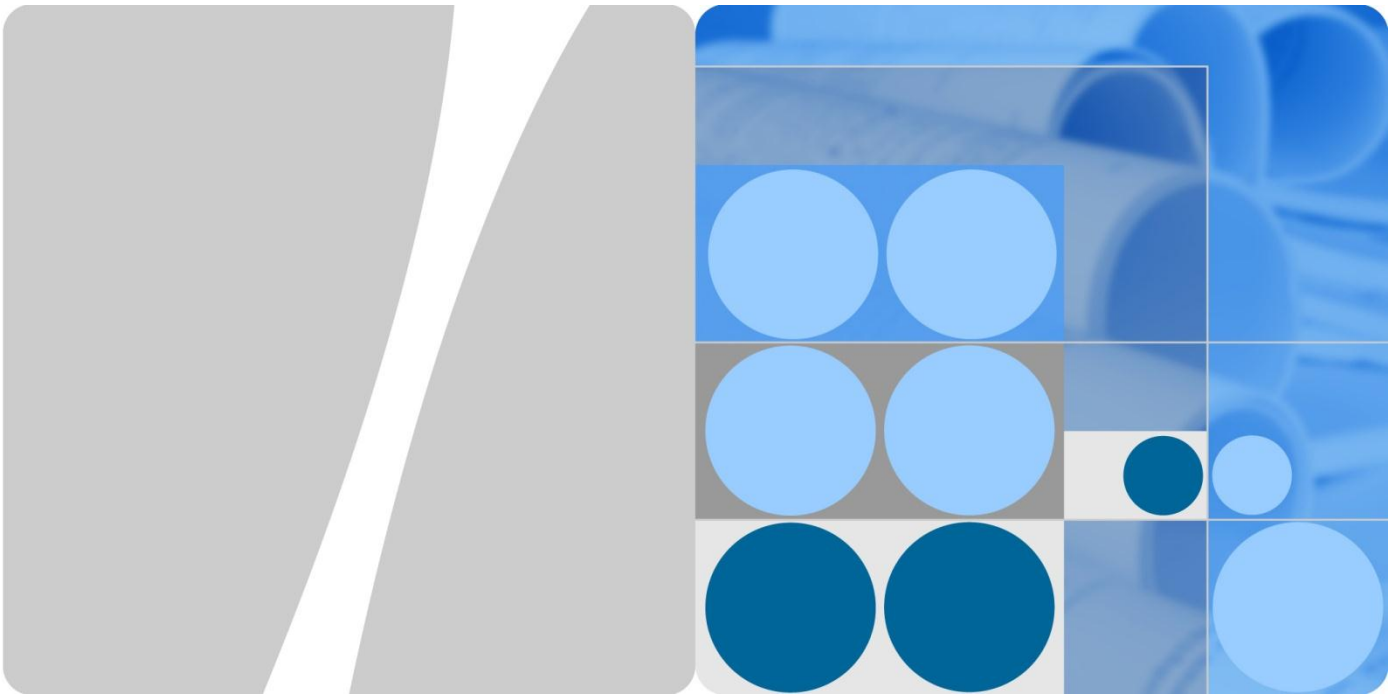

# 华为 ASG2000 上网行为管理产品
# 技术白皮书

华为技术有限公司

**版权所有 © 华为技术有限公司 2012。 保留一切权利。**

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

**商标声明**


和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

**注意**

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

# 华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

# 目 录

# ASG 技术白皮书

## 1 技术背景

在Internet飞速发展的今天，网络已成为企业的重要生产工具，员工通过网络可以查找资料、沟通交流和从事电子商务等，但是相应的多种问题伴随而生，例如：

- 与工作无关的 P2P 和在线视频等应用占用带宽
- 与工作无关的聊天、炒股、游戏、博客和在线购物等活动影响工作效率
- 员工随意在网络上发帖和传输文件导致机密泄露
- 员工上网容易受到病毒、木马和蠕虫等攻击和感染
- 员工通过网络从事一些黄赌毒等违法活动
- 员工浏览和发布不良言论导致企业面临法律风险

为解决以上一系列的问题，上网行为管理产品应运而生，华为凭借在应用识别库和网络安全等全方面的多年积累，推出了专业级的上网行为管理产品ASG。ASG设备可实现员工上网行为的管理、带宽的限制和确保员工上网安全等，可以极大提高员工的办公效率和带宽利用率，防止机密数据泄密和员工通过网络从事违法活动。

ASG（Application Security Gateway）是华为技术有限公司（以下简称华为）推出的上网行为管理产品，主要解决内部员工上网带来的工作效率低下、带宽滥用、恶意软件感染、内部信息泄漏以及法律合规等问题。

## 2 上网行为管理给用户带来的价值

ASG是华为在充分了解客户和市场需求的基础上，通过成熟的系统设计推出的上网行为管理产品，具有精准的应用识别、电信级高可靠性、全面威胁过滤和专业报表等特点。

ASG2000系列产品，是业界应用识别最丰富，威胁防护最全面的上网行为管理产品。该系列产品提供URL过滤、应用行为控制、流量管理、数据防泄漏、恶意软件防护、互联网行为记录等多项功能，为企业机构提升员工工作效率、营造安全办公环境、以及法规遵从提供了一体化的解决方案。

ASG2100/2200

ASG2600/2800

## 2.1 最丰富的应用识别，更好地提升办公效率

员工在互联网上进行一些与工作无关的活动将导致工作效率低下，增加企业的人力成本。ASG可以通过丰富的特征库协助企业解决此类问题。

在网络快速发展的今天，新型应用层出不穷，URL站点变化频繁，当应用和URL站点增加、减少和变更时，华为会在第一时间更新特征库，提高识别准确率。华为具有专业的应用特征库和URL分类库研发团队，密切跟踪全球应用和URL变化，积累了国内第一、国际领先的应用特征库和URL库：

- 安全服务中心提供超过1200种的应用识别，覆盖企业网络主流应用，如P2P、在线视频、流媒体、股票行情、网络游戏和网络存储等。
- 安全服务中心提供超过 6500 万条的海量 URL 库，细分为百余种类别，涵盖工作无关网站，木马、钓鱼和恶意软件网站，以及黄赌毒等不良站点。
- 特征库更新频率快，让用户在最短时间内获得最新的特征库。

通过丰富的应用识别库，精准识别用户访问的应用协议，并通过对不同的应用协议采取合适的动作，从而更好地管理员工上网行为、提高办公效率。

## 2.2 全面的内容控制和审计，有效防止信息外泄和协助法规遵从

ASG通过多种方式的内容控制防止敏感信息外泄和员工发布违反法律法规的不良言论，全面的审计功能为事后审查提供有力证据。

ASG支持主要内容外发方式的内容控制，实时过滤非法信息外传：

- Web 内容控制包括提交内容关键字过滤（禁止关键字内容对外发布）和 HTTP 协议、FTP 协议文件外传控制。
- 邮件内容控制包括限制发件人和收件人，邮件内容关键字过滤（禁止关键字内容邮件发送）和附件外发控制。
- IM 软件内容控制通过管理员配置的文件大小和文件类型限制内网用户通过 IM 软件外发文件。

ASG支持全面的内容审计，协助企业事后审查：

- Web 审计
  - 记录用户访问的 URL
  - 记录用户通过网页上传的文本内容
  - 记录用户通过 HTTP 方式外发的文件名称、大小和类型，对于不大于 10M 的外发文件，还支持保存小于指定大小的原始文件
  - 记录用户通过 HTTP 方式下载的文件名称、大小和类型
- IM 软件审计
  - 支持对 QQ、阿里旺旺、飞信、MSN、雅虎通和 Gtalk 软件的审计。审计内容包括记录聊天内容和外发文件的属性，对于不大于 10M 的外发文件，还支持保存原始文件。
- 邮件审计

- 对于企业员工发送的邮件，记录发件人、收件人、邮件标题、邮件正文和附件的名称、大小、类型，对于不大于 10M 的附件，还支持保存小于指定大小的原始文件。
- 对于企业员工接收的邮件，记录记录发件人、收件人、邮件标题、邮件正文和附件的名称、大小、类型。

## 2.3 四重保护上网用户，恶意软件无所遁形

针对用户上网面临的威胁，提供多重防护确保上网安全。用户上网时面临着各种安全威胁，如钓鱼网站、网页木马、文件病毒、黑客攻击等，ASG产品提供全方位的防护措施，具备多重防护能力，确保用户上网安全。

- 迅速感知新的恶意站点，防止用户因访问这些网站遭受财务诈骗、私密信息泄漏等。
- 基于业界领先的赛门铁克专业防病毒引擎，实现高达 99%的病毒检测率。
- 基于漏洞利用和启发式检测引擎，有效防御未知恶意软件和各种变形攻击行为。
- 检测用户机器被黑客操控以及通过木马外传信息等异常流量行为，并及时阻断。

## 2.4 专业报表针对性强，助力企业治理

ASG提供带宽利用、工作效率、法律合规和威胁过滤等丰富的报表，协助企业进行上网业务运维、发现上网问题和完善内部管理，辅助企业在上网方面的管理和投资决策。

ASG通过B/S架构的专业管理中心进行日志、报表管理。
支持访问网站日志、邮件日志、文件外传日志、异常行为日志和流量日志等多种日志明细查询。

专业的报表系统提供统计报表、趋势报表、对比报表和综合报表四种报表形式，并且支持多种输出格式，同时具有柱状图、饼状图和曲线图等丰富的呈现方式。

- 统计报表
  提供上网时长、上网流量、上网行为和网络威胁统计报表，可以从用户、部门和应用类型等多维度分别展示办公效率、带宽利用和威胁过滤方面的整体情况。
- 趋势报表
  提供上网流量和上网行为的趋势分析报表，可以从用户、部门和应用类型等多维度展示办公效率和带宽利用率的发展趋势。
- 对比报表
  提供上网流量和上网行为的对比分析报表，可以对比分析基准日期和前一天、上一周、上一月部门员工上网流量和访问指定类型网站次数，展示办公效率和带宽利用率的对比情况。
- 综合报表
  提供综合报表，展示用户在办公效率、带宽利用、威胁过滤和合规性方面的总体概况和专项评估情况，以辅助管理和投资决策。

## 2.5 丰富附加功能，提升产品价值

ASG内置电信级状态检测防火墙对进出组织的数据包进行过滤，提供NAT代理内部员工上网，提供NAT-SERVE功能将内部服务器映射到公网地址，可扩展Wifi模块实现本地无线接入、为小型企业或分支机构客户节省客户成本和简化网络部署。

## 2.6 电信级高可靠性，为业务保驾护航

ASG产品通过设备级和网络级的多种可靠性手段来保证业务的连续性。

### 2.6.1 设备级高可靠性

ASG按照电信级产品可靠性要求，采用专门设计的硬件系统，可长期运行于温度0℃～45℃，湿度10%RH～90%RH（无冷凝）的恶劣环境中。此外，ASG2600/2800支持温度监控、风扇热插拔，电源模块采用双电源（1＋1备份），两个电源模块可以互相热备份，并且支持热插拔，电源倒换时不影响系统运行。

### 2.6.2 网络级高可靠性

**双机热备**

- ASG 支持双机热备份组网，支持 HRP（Huawei Redundancy Protocol）协议，双机热备包括主备备份和负载分担两种方式。
- 主备备份方式组网时，一个备份组内包括一个主用设备和一个备用设备。HRP 协议负责在主/备设备之间备份关键配置和会话表状态信息，从而确保主用设备出现故障时能由备用设备平滑地接替工作。
- 负载分担方式组网时，两台设备互为主备，正常情况下两台设备同时处理业务。当其中一台设备发生故障时，另外一台设备会立即承担其业务，保证原来需要通过这台设备转发的业务不中断。相对于主备备份方式来说，主用设备和备用设备共同处理业务流量，可以提高网络的转发效率，降低主用设备发生故障的几率。

**硬件Bypass**

- ASG2600/2800 支持插入电 Bypass 接口卡和光 Bypass 接口卡，当设备出现故障时，Bypass 接口卡将上下游设备直接相连，保证业务不中断；当故障排除后，所有流量恢复由设备处理后再发送，保证业务的安全性。

**软件Bypass**

- 启用软件 Bypass 功能后，ASG 不对业务做控制和审计，相当于上下游设备直接连接。

**引擎失效、过载保护**

- 当 URL 分类过滤、恶意流量检测、病毒检测和内容过滤等引擎失效或者过载后，将未能通过这些引擎检测的流量直接放行，确保业务不中断。

# 3 ASG 技术简介

华为技术成立至今拥有大量的技术专利，这些专利技术使得华为技术的各项产品一直领先于业界的同类产品。本章节将向您介绍一些切实能带给您便利和解决您问题的技术，阐述ASG如何实现全面而灵活的上网行为管控与审计。

## 3.1 用户管理

ASG除了支持本地用户系统，还支持跟第三方用户系统进行联动，包括从第三方系统导入用户和与第三方系统联动实现用户认证，支持导入用户的第三方系统包括AD域服务器、TSM（华为终端安全管理系统），支持联动实现用户认证的第三方系统包括AD域服务器、TSM、标准的Radius认证服务器。

### 3.1.1 从第三方系统导入用户

一个大中型企业动辄几百上千人，管理这些人员的账号信息，无疑是一项非常大的工作。ASG支持从第三方系统导入用户信息，使得管理员在自己网络里同时部署多套系统的时候，只需要维护一套用户信息，这一特性大大的简化了管理员的运维成本。

ASG通过使用标准的LDAP协议与AD域服务器通讯，从AD域服务器获取organizationalUnit对象作为部门，获取Person对象作为用户，并且将导入到本地的部门保持与AD上同样的树状结构。

从TSM导入用户时，由ASG设备通过http协议主动向TSM请求部门和用户数据。ASG与TSM之间通讯的协议内容是使用xml封装后使用3des算法进行加密的，属于内部协议。

### 3.1.2 单点登录

单点技术(Single Sign On, SSO)将避免用户重复输入帐号密码的繁琐操作。ASG不但能支持与AD服务器联动进行单点登录，还能与TSM服务器联动进行单点登录。

**AD单点登陆的流程如下：**

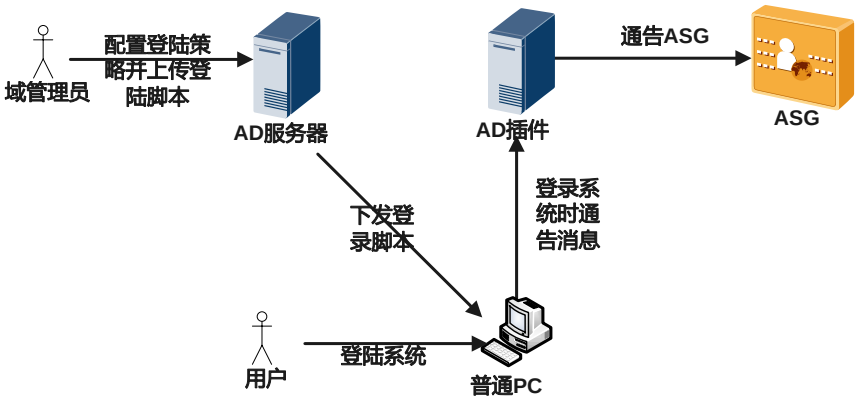


图1. AD单点登录

要使用AD的单点登录，AD域的管理员需要先对AD域进行策略配置，在策略上给用户设置ASG的单点登录脚本。

当用户使用AD域的用户登录操作系统时，域控制器将会自动将ASG的登录脚本下发到已经加入AD域的PC机器上，登录成功后，ASG的登录脚本会自动执行，执行后，ASG登录脚本自动与ASG的AD插件（可以直接安装在AD域服务器上）通讯（通讯包围通过3DES加密），AD插件确认用户登录后，通过UDP协议（ASG内部协议）将用户登录消息通知ASG设备，ASG设备这个时候让用户在本地上线。

TSM单点登录：

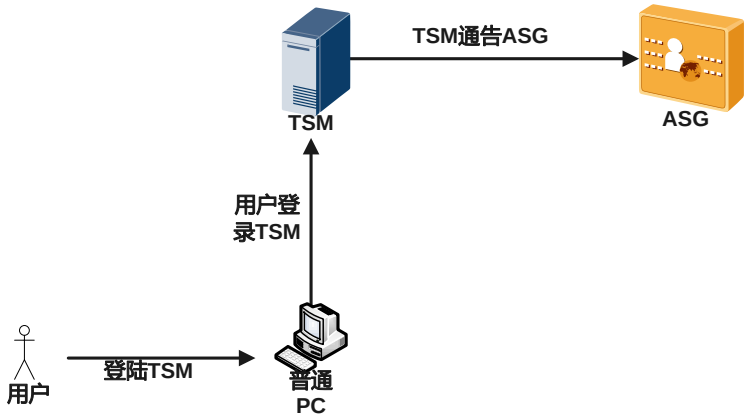


图2. TSM单点登录

用户进入系统后，使用TSM Agent输入用户名密码或者TSM Agent自动登陆TSM系统，登录成功后，TSM系统通过UDP协议（ASG内部协议）将用户登录的消息通知ASG设备，ASG设备这个时候让用户在本地上线。

TSM的用户成功状态包括认证通过、安全认证通过，两种状态的变动都会通知ASG设备，ASG收到消息后会根据本地设置来让用户上线和下线。

### 3.1.3 旁路强制认证

ASG的网络准入控制能够支持通过对客户端进行强制认证来实现网络的访问控制从而更好的保证网络的安全。

在旁路模式下，用户没有认证通过前，ASG可以对TCP流量进行阻断，对于HTTP协议支持推送页面，强制用户进行认证。对于TCP阻断的原理如下：

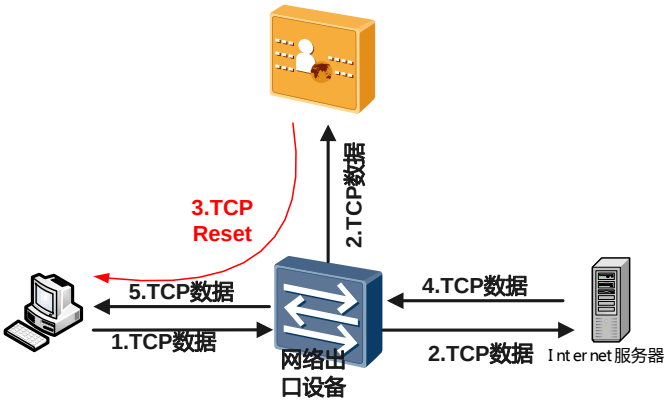


图3. 旁路阻断原理

如上图，从内网机器向外网发送的TCP协议数据到达网络出口设备时，在正常转发数据包的同时也会给ASG镜像一份，当ASG收到这个报文时，发现用户没有登录，会马上给内网的机器回复一个带Reset标志的TCP报文，内网机器收到该报文后会关闭连接。

从图中可以看到，报文3必须要在报文5前到达内网的机器，否则报文3会由于TCP序列号不正确而被抛弃。

目前ASG仅在机器未登陆时控制TCP的连接，登陆后不进行策略控制TCP连接。

对于HTTP的推送，原理是一致的，就是在收到TCP包的时候就开始进行TCP劫持（从技术上也可以认为是TCP欺骗）然后返回HTTP重定向URL由web浏览器自动跳转到认证页面。目前HTTP重定向仅支持80端口。

## 3.2 应用控制和 URL 过滤

企业或者组织接入互联网的带宽一般非常有限。当这个有限的带宽充斥了大量的无关应用（如在线游戏、P2P和在线视频）的时候，一些重要应用将受到挤压，基本带宽得不到保证，使得网络对于工作和重要业务不再可用。

ASG通过DPI（Deep Packet Inspection），即深度报文检测技术，对数据流中的应用层数据进行内容检测。对通过解析的数据包，使用应用特征库中的规则，对应用数据进行匹配，分析报文或流在IP和UDP/TCP层以上的应用类型。

ASG对应用的识别方式并不是传统的基于端口的方式来识别，而是使用应用特征库来识别，通过分析经过设备的网络数据包，并和应用特征库进行比对，识别出在线游戏、P2P和在线视频等多种类型的网络数据流量，然后根据用户对该类应用配置的动作允许还是阻断数据包。

华为提供丰富的应用特征库，能够准确识别网络中的主流应用，同时支持自定义应用对应用特征库进行补充和实现用户个性化设置。

URL过滤在企业中是非常重要的功能，ASG提供了非常丰富的URL分类库，由于ASG所支持

的URL库非常庞大（总数量达到几千万），并且是实时更新的，ASG除了采用了两级查询技术，用于提高将URL分类的速度，第一级是ASG设备本地的缓存，本地缓存包括本地内存中的高速缓存和本地持久性存储里面的URL库，第二级是华为提供的URL分类库服务器，URL分类库服务器是在Internet的一个强大的服务器，含有几千万条URL信息，并且可以实时更新URL以及分类信息。URL分类查询的过程如下：

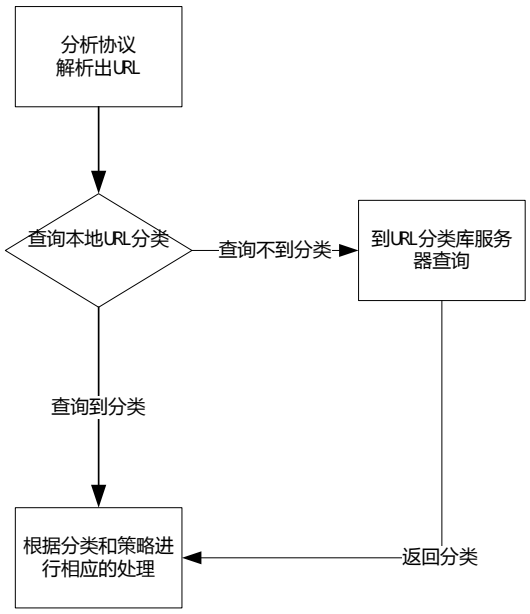


图4. URL分类查询流程

本地缓存的URL数量是有限的，在到URL分类库服务器查询到分类后，ASG设备会根据URL的使用频率和使用时间等对本地缓存的URL库进行优化，使得ASG设备在经过一段时间运行后，绝大部分URL都可以直接在本地查询到，提高查询速度。

如果ASG设备无法连接到URL分类库服务器服务器，那么只能使用本地的URL缓存。

应用控制和URL过滤在ASG系统中属于上网权限策略。

## 3. 3　流量管理

### 3.3.1　基于 IP 地址（地址段）的流量控制

IP（段）的流量控制是指根据报文源地址、源端口、目的地址、目的端口、协议这五元组信息匹配限流策略，如果匹配上了则进行相应的限流，否则不做限流。策略里面可以配置地址或地址的集合，协议或协议的集合，配置起来很方便。

针对IP（段）的流量控制，支持两种方式：

- 每IP限流：对每个内网地址进行限流；
- 总体限流：对命中策略的所有流量进行限流；

比如：某网络要对172.16.1.1-172.16.1.200的用户配置每个IP限制1M，整体限制150M。

### 3.3.2 基于 DPI 应用的流量控制

DPI(Deep Packet Inspection)作为一种较新的包检测技术，除了能够检测P2P、IM，还可以识别包括VOIP（skype、H.323、SIP、RTP、Net2Phone、Vonage），Game（Diablo、Tantra），web_Video（PPlive、QQlive、SopCast），Stock，Attack等20多种大类，以及上千种应用协议，该DPI库支持在线升级，保证DPI库的实时更新。

用户根据DPI应用类型分别采取不同的限流策略，比如对迅雷业务每个用户进行限速1Mbps，整体迅雷业务限制10Mbps，对于http业务则不限制。基于DPI应用的流量控制可采用的控制策略包括：

- 允许通过：即允许该应用流量通过。
- 禁止通过：即禁止该应用流量通过，对于被禁止的流，ASG对应的会话表会保留一定时间，防止会话老化后重新识别时因为后续包没有特征而无法准确识别出来，致使后续报文而又能通过。
- 带宽限速：对该种类型应用流量进行限速。
- 连接数限制：对该种类型应用的连接数进行限制，防止该类应用占据系统的连接数资源。

例如：某小区网络中迅雷流量占据了很大出口带宽，在业务高峰6:00-22:00时，迅雷业务飙升，占据了大量带宽，使得访问web网页也很慢，为了解决这个问题，可以通过配置对每个用户IP的迅雷限流500Kbps，同时对整体的迅雷做200Mbps限流，防止迅雷业务流量过大对整个网络的冲击。

### 3.3.3 基于用户（部门）的流量控制

随着Web2.0的发展，由于网络结构的分散和网段、地址的不固定性，传统设备基于对IP网段限流策略的固定配置，已经不适合当前网络动态发展的需求，因此，企业存在着对业务流量进行基于用户（部门）识别和基于用户（部门）配置限流策略的需求。

在流量识别对应用户身份的基础上，ASG只需要针对用户（部门）信息配置限流策略，而不再需要根据复杂多变的IP网段来进行限流配置，这样不同的用户（部门）身份可配置不同的流量控制策略，既简化了策略配置，又适应了企业复杂多变的网段规划，方便管理员的管理。

例如：企业总出口带宽10M，部门A和部门B的用户访问外网internet业务时，针对部门A中迅雷业务限制为每员工100Kbps；而部门B中每员工限制http上网业务200Kbps；另外，对于

特权用户（如总经理）配置优先带宽2M。

### 3.3.4 支持对流量进行双重控制

双重控制是指可对流量同时进行两种方式的限流：

- 每IP/用户限流：域间配置，具有方向性，针对每个IP/用户进行限流。
- 总体限流：域间配置，具有方向性，针对命中匹配策略的流量进行总体限流。

例如：企业总出口带宽10M，部门A和部门B的用户访问外网internet业务时，针对部门A中每个用户的迅雷业务限制100Kbps，同时配置部门A所有员工共享的总出口带宽为2M；而部门B中每个用户限制http上网业务200Kbps，限制部门B所有员工总带宽为6M；另外，对于特权用户（如总经理）配置优先带宽2M。

### 3.3.5 支持对流量进行保证带宽控制

保证带宽：是指每个IP地址保证能够通过的流量，当总体带宽有空余时，则每个IP地址能够通过大于保证带宽值，而小于最大带宽值的流量。对于大于保证带宽的报文，转发还是丢弃是按照报文到达时带宽是否超过总体带宽来决定，超过时则丢弃，否则转发。

最大带宽：是指配置保证带宽功能后每个IP最大能够通过的带宽，当超过这个最大带宽时，报文直接会被丢弃。

总体带宽：是指出口整体带宽的值，一般是设置为（保证带宽*用户数）。

例如：某网吧共有100个用户，出口总带宽为100M，那么每个用户可以保证的带宽值为100M/100 = 1M, 最大带宽则可以设置的比保证带宽要大，比如为5M。

当只有10个用户上线时，每个用户至少保证1M能够通过，最大允许通过5M流量。

当100个用户全部上线时，则每个用户至少保证1M流量能够通过。

### 3.3.6 支持对流量进行连接数控制

连接数的限制是指对并发连接数进行限制，现网应用P2P等占用了很多连接资源，对连接数进行限制，从而达到对流量进行限制目的。

- 每IP并发连接数限制：针对每个IP地址限制并发连接数个数，对于超过这个规则的连接将会被阻断。
- 整体并发连接数限制：针对命中策略的并发连接数的总和进行限制，对于超过规则的

连接将会被阻断。

比如：某公司局域网为了防止个人上网占用连接数太多，下载流量太大，则对每个人的并发连接进行限制100条，整体限制10000条。

## 3.4 行为和内容审计

用户在互联网的上网行为直接关系到企业的网络管理的成本。滥用带宽、网速奇慢；网络病毒泛滥、攻击频繁；发布不良言论，给企业管理带来麻烦。有效的审计能够帮助企业快速定位到问题的根结，帮助企业高效的解决问题。

ASG可以对绝大部分的网络行为进行审计，包括

- 应用审计

  审计应用的分类、应用名、使用该应用的用户、用户所在部门、目的地址、应用流量、应用使用时长等。

- 知名端口非标协议审计

  审计常见端口（21、25、80、110和443端口）上的非标准协议流量，以识别潜在风险。

- URL访问审计

  审计域用户所访问的URL，支持审计所有URL和仅审计指定分类的URL。

- Web内容上传审计

  审计用户通过HTTP协议POST的内容，供事后追查在论坛/博客上发表的不良言论。

- Web文件外发审计

- 审计用户通过HTTP协议上传的文件，有效追踪泄密事件。Web文件下载行为审计

  审计用户通过网站下载的文件名称、类型和大小，了解用户下载行为。

- 邮件审计

  支持审计邮件标题、邮件内容、发件人、收件人、邮件附件等。

- IM聊天审计

  IM审计需要使用ASG客户端，可以审计的IM软件包括QQ、阿里旺旺、飞信、MSN、雅虎通和Gtalk，可以审计聊天内容和外发的附件。

## 3.5 内容过滤

除了审计，ASG还能够对用户外发的内容进行过滤，防止涉及知识产权或企业机密的信息外泄。

- Web 内容控制

Web 内容控制可以对 HTTP 协议传输的 Web 页面内容和附件进行控制，可以控制的项目包括：

- Web 文本内容提交过滤：按关键字过滤内网用户通过 Web 页面提交的文本（如 BBS、论坛发帖），并控制提交文本内容的大小。
- 文件外传控制：通过文件大小和文件类型控制 HTTP 方式和 FTP 方式的文件外传。
- Web 浏览关键字过滤：内网用户通过浏览器浏览 Web 页面时，按关键字过滤 Web 页面上的文本。

- 邮件外发控制

邮件外发控制可以对 SMTP 邮件和 Webmail 实现邮件发件人、收件人、邮件标题和内容以及邮件附件的控制：

- 发件人和收件人过滤：允许或者禁止指定邮件地址的发件人发送邮件、收件人接收邮件。
- 标题和正文过滤：按关键字过滤发送邮件的内容。
- 附件过滤：按附件大小、个数和文件类型过滤发送邮件的附件。

- IM 控制

ASG 支持对多种 IM 即时通信软件进行监控，启用 IM 监控需要启动 ASG 客户端，如果要强制进行 IM 监控，可以强制使用 ASG 客户端。

IM 监控使用了多种技术，监视监控某 IM 通信工具外发聊天信息的原理如下：

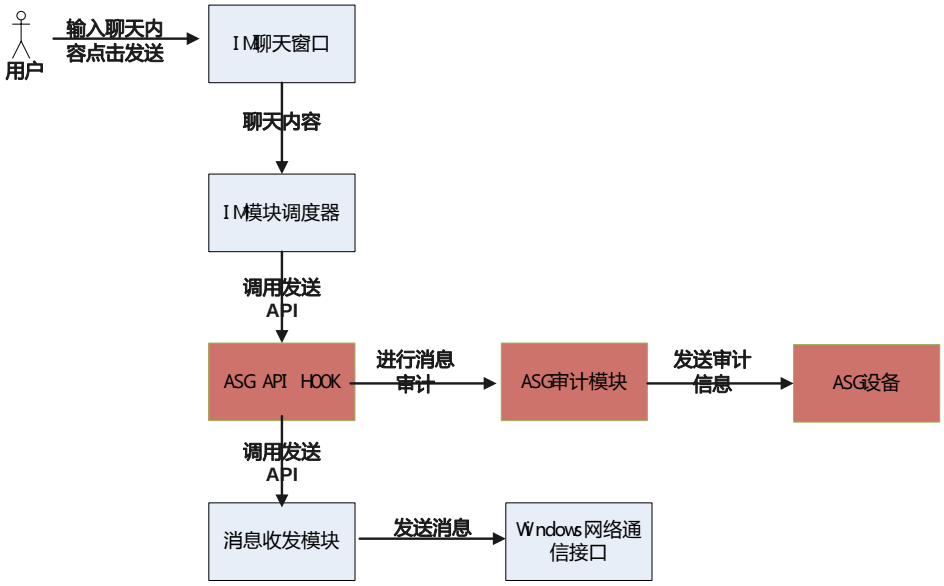


图5. IM审计原理

## 3.6 威胁防护

大多数企业均面临着恶意软件的威胁，IDC预计75%的办公电脑在不知情的情况下感染了间谍软件，间谍软件和其他类型的恶意软件可能导致机密信息外泄、办公电脑或网络故障、降低员工工作效率、以及昂贵的桌面维护成本。

ASG提供业界最为先进的恶意流量检测技术和病毒检测技术，可以识别变形和新型攻击，有效抵御针对上网用户的恶意软件威胁。

### 3.6.1 基于签名的恶意流量检测技术

通过对已知的攻击行为进行特征提取形成表示该特征的唯一签名，之后将这些签名放入签名库中，当IPS将网络数据进行重组后，将数据流与这些签名进行某种比较和匹配操作(关键字、正则表达式、模糊近似度等)，从而发现可能的网络攻击行为，因此基于特征检测的方法准确率高。

此外由于恶意流量检测只需要对数据报文进行特征匹配即可，对于应用层攻击的检测实际上是通过对3层报文的扫描实现，具有很高的检测效率。随着出现新的攻击软件或者攻击软件进行升级之后，对应的恶意流量检测的规则也需不断更新。

华为 ASG的恶意流量检测功能支持基于签名的特征检测，签名库规格大于2500条，提供高品质的攻击特征介绍和分析，基于高速、智能模式匹配方法，能够精确识别各种已知攻击，包括病毒、特洛伊木马、蠕虫病毒等，并通过不断升级攻击特征，能够迅速检测到攻击行为。

华为公司通过与赛门铁克公司的深入合作，利用赛门铁克的专业安全团队密切跟踪全球知名安全组织和软件厂商发布的安全公告，对这些威胁进行分析和验证，生成保护各种软件系统（操作系统、应用程序、数据库）漏洞的特征库；此外，通过赛门铁克遍布全球的蜜罐系统，实时捕获最新的攻击、蠕虫病毒、木马等，提取威胁的签名，发现威胁的趋势。华为 ASG能够在最短时间内获取最新的签名，及时地获取最新的IPS引擎，从而具备防御零日攻击的能力。

华为 ASG的恶意流量检测功能升级方式分为以下几种（与IPS签名库升级基本相同），分别适用与不同的操作场景：

- 自动定时升级：更新及时，能第一时间对新产生的攻击进行防御，且不需要用户干预操作，比较适用于能连接到升级服务器的设备。如果需要确认新下载的签名库是否安全可用，可以采用确认机制，定时下载新版本，但不立即应用，确认后应用。
- 实时升级：当可能有新版本发布，但未到自动升级的时间的时候，可以手工进行定时升级，优点是实时性高，且能立刻知道升级结果。
- 本地升级：当设备无法与升级服务器建立连接或者需要将版本回退到较早之前的一个版本的时候，可采用本地升级，将版本切换到本地升级指定的版本。
- 版本回退：可回退到上一个正常应用的版本。如果发现当前版本可能误报率较高，检测率较低或者其它不合理的因素时，可将版本回退到上一个正常应用的版本。

### 3.6.2 基于特征码的病毒检测技术

特征码扫描是目前国际上反病毒软件普遍采用的查毒技术。其核心是从众多电脑病毒中提取病毒特征码，构成病毒特征库。病毒特征码是该病毒所特有的一系列二进制串，可以将病毒同其它病毒或正常程序区别开来。反病毒引擎将提取的文件或者数据，与病毒特征库中的特征码逐一比对，从而判断该目标是否被病毒感染。

华为 ASG的病毒特征库非常丰富，包含了3万条以上的病毒特征，包含了绝大多数当前最新的、恶性病毒的特征码，能够有效地检测出病毒。

华为通过与赛门铁克公司的深入合作，利用赛门铁克的全球分布病毒监控网点和专业的病毒

分析团队，华为 ASG能够在最短时间内获取最新的病毒特征，及时地获取最新的反病毒引擎。升级方式分为以下几种（与IPS签名库升级基本相同），分别适用与不同的操作场景：

- 自动定时升级：更新及时，能第一时间对新产生的攻击进行防御，且不需要用户干预操作，比较适用于能连接到升级服务器的设备。
- 实时升级：当可能有新版本发布，但未到自动升级的时间的时候，可以手工进行定时升级，优点是实时性高，且能立刻知道升级结果。
- 本地升级：当设备无法与升级服务器建立连接或者需要将版本回退到较早之前的一个版本的时候，可采用本地升级，将版本切换到本地升级指定的版本。
- 版本回退：可回退到上一个正常应用的版本。如果发现当前版本可能误报率较高，检测率较低或者其它不合理的因素时，可将版本回退到上一个正常应用的版本。

## 3.7 审计与报表

ASG系统对多种用户数据进行审计，用户数据主要来源于2个位置，ASG设备与ASG客户端，ASG设备通过协议分析对网络报文分析等技术识别用户行为和分析内容，ASG客户端将审计到的数据先发送到ASG设备，有ASG设备再发送到日志采集器。

报表不是对源数据进行统计，而是在日志采集器先经过一次初步的统计，然后报表模块利用初步统计的数据进行二次统计而得出的结果。

报表系统是ASG Manager中最重要并且最复杂的系统，为了提高性能，报表系统对于各种统计数据进行分钟表、小时表、天表的分表处理。

ASG数据审计到的数据流向如下：

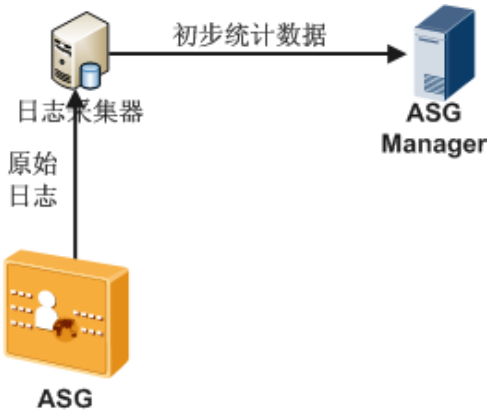


图6. ASG设备的日志处理过程

ASG客户端审计到的数据流向如下：

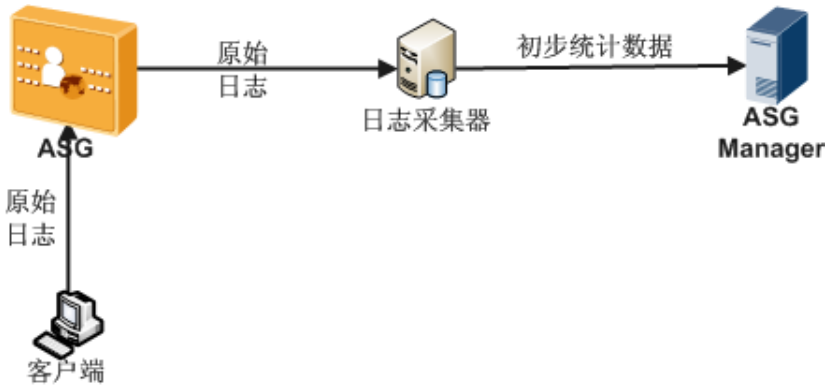


图7. ASG客户端日志处理过程

# 4 部署您的 ASG

作为一款充分了解客户和市场需求的上网行为管理设备，ASG提供了丰富的部署模式能够满足不同的网络环境和用户需求。

## 4.1 网桥模式

**单网桥**

ASG与内网交换机连接的接口加入LAN区域，与出口网关连接的接口加入WAN区域，形成一进一出单网桥组网。ASG对内网用户的上网行为进行管理，并提供审计功能。

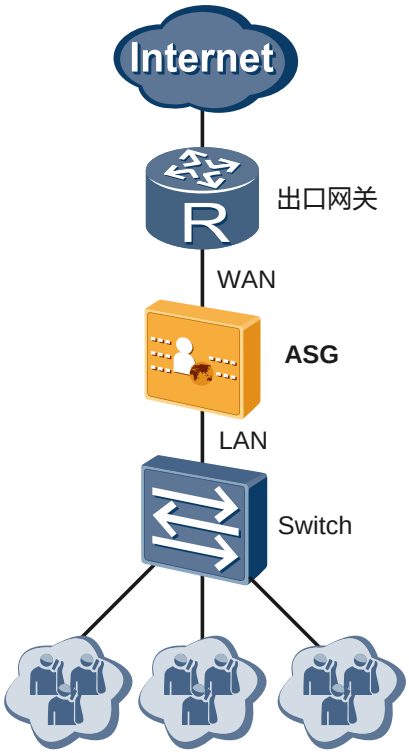


图8.单网桥

适用场景：企业具有出口网关，不希望改动现有网络环境

硬件要求：一台ASG2100/ASG2200/ASG2600/ASG2800，ESP卡或者一台PC服务器（用于部署ASG Manager）

软件要求：在选用独立PC服务器部署ASG Manager时需要单独提供Windows 7/Windows 2003/Windows 2008

**多网桥**

ASG支持多个网桥，可以通过指定不同的LAN/WAN口进行配置，不同网桥之间在设备内部通过VLAN进行隔离。ASG还支持网桥多网口，即一个网桥中包含多对多或一对多的接口，这些接口属于同一个VLAN，可以相互通信。

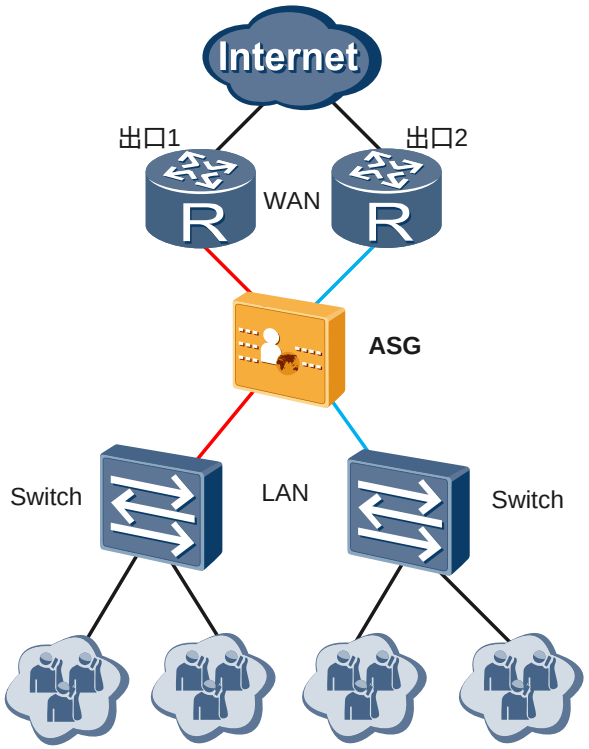


图9.双网桥

适用场景：企业网络被隔离为多个，并且都具有出口网关，希望仅适用一套ASG设备进行管理，不希望改动现有网络环境

硬件要求：一台ASG2100/ASG2200/ASG2600/ASG2800，ESP卡或者一台PC服务器（用于部署ASG Manager）

软件要求：在选用独立PC服务器部署ASG Manager时需要单独提供Windows 7/Windows 2003/Windows 2008

## 4.2 网关模式

**单ISP**

网关模式的ASG工作在三层，通常部署在企业网络出口处，作为出口网关。网关模式组网通常还启用源NAT，将上网PC的私网IP地址转换为公网IP地址。

网关模式组网支持所有的业务功能，尤其对NAT功能支持全面，同时支持源NAT和地址映射（虚拟服务器）。

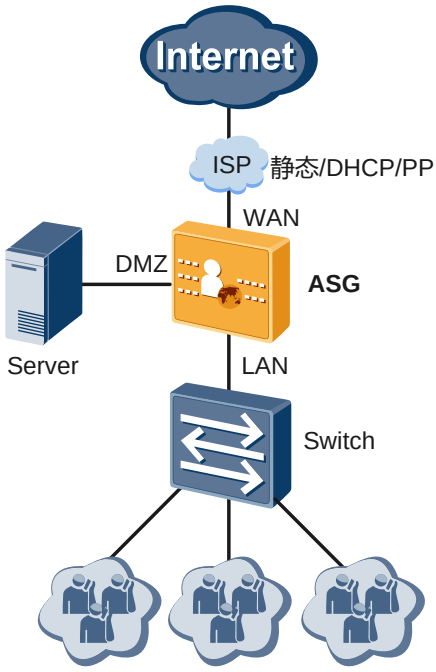


图10.　网关模式-单ISP

适用场景：企业没有出口网关，需要使用ASG做出口网关，只接入一个ISP

硬件要求：一台ASG2100/ASG2200/ASG2600/ASG2800，ESP卡或者一台PC服务器（用于部署ASG Manager）

软件要求：在选用独立PC服务器部署ASG Manager时需要单独提供Windows 7/Windows 2003/Windows 2008

**多ISP**

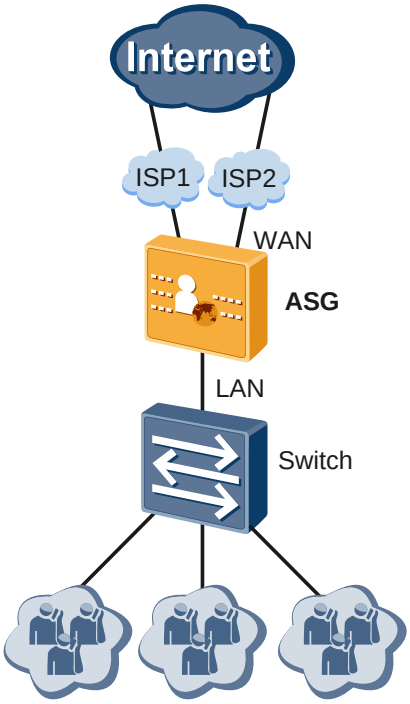


图11.　网关模式-多ISP

适用场景：企业没有出口网关，需要使用ASG做出口网关，只接入多个ISP

硬件要求：一台ASG2100/ASG2200/ASG2600/ASG2800，ESP卡或者一台PC服务器（用于部署ASG Manager）

软件要求：在选用独立PC服务器部署ASG Manager时需要单独提供Windows 7/Windows 2003/Windows 2008

## 4.3　旁路模式

旁路模式通过交换机或HUB的流量镜像功能把用户的上网数据镜像到ASG，从而实现对上网行为的审计。旁路组网时即使ASG发生故障也不会影响网络业务。

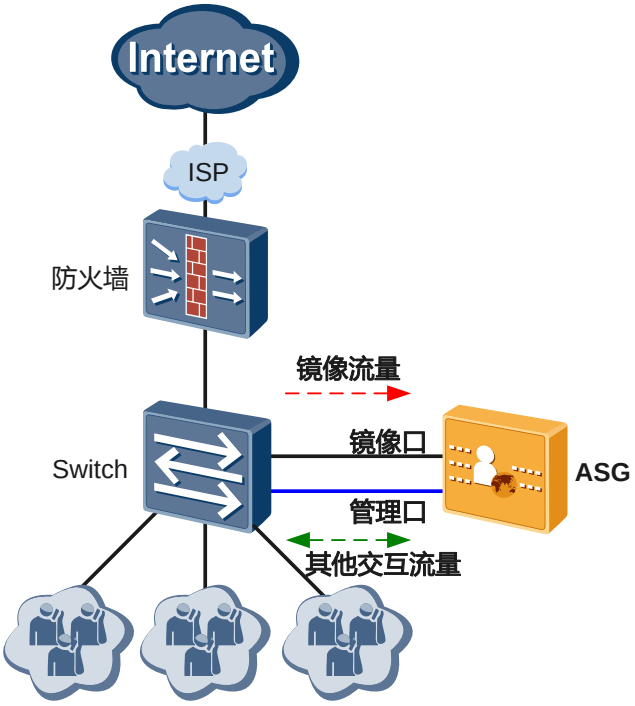


图12.　旁路模式

适用场景：企业具有出口网关，不需要对网络进行改造，对上网行为的审计具有要求，对用户行为的权限控制基本没有要求或者仅要求身份认证。

硬件要求：一台ASG2100/ASG2200/ASG2600/ASG2800，ESP卡或者一台PC服务器（用于部署ASG Manager）

软件要求：在选用独立PC服务器部署ASG Manager时需要单独提供Windows 7/Windows 2003/Windows 2008

# 5　产品列表和规格

| 型号 | ASG2100 | ASG2200 | ASG2600 | ASG2800 |
|---|---|---|---|---|
| **性能** | | | | |
| 应用场景 | 分支机构/SMB | 分支机构/SMB | 大中企业 | 大中企业 |
| 性能定位 | 低端百兆 | 标准百兆 | 低端千兆 | 标准千兆 |
| **网络接口** | | | | |
| 默认接口 | 4GE+2Combo | 4GE+2Combo | 4GE+4Combo | 4GE+4Combo |
| 扩展接口 | 4MIC+1FIC | 4MIC+1FIC | 2FIC | 2FIC |
| 扩展接口卡 | MIC-1FE、MIC-5FE、MIC-WiFi、FIC-4GE、FIC-1GE | | FIC-8GE、FIC-8GE（光）FIC-4GE Bypass、FIC-2路光口bypass | |
| **主要功能** | | | | |
| 应用识别 | 识别IM、P2P、流媒体、网络游戏、炒股、Webmail、网络存储、网络隧道等1200+应用，如：QQ，MSN，PPStream，Youtube，迅雷，电驴，魔兽争霸、同花顺，大智慧、纳米盘等等。支持300+种移动智能终端应用识别 | | | |
| URL分类 | 6500万+URL库，云端自动更新 | | | |
| 用户识别 | 设备内置账号、外部AD/LDAP、外部Radius、TSM等 | | | |
| 认证机制 | 手动认证（Web认证、终端认证）、自动认证（AD/TSM单点登录、网段认证） | | | |
| 应用控制 | 基于用户、时间、应用/URL分类等因素，提供灵活的控制策略 | | | |
| 流量管理 | 基于用户、应用/协议、时间、链路、带宽等多维度调控手段，带宽保证和限制 | | | |
| 数据防泄漏 | 外发内容过滤、审计，外发文件过滤、审计 | | | |
| 恶意软件防护 | 信誉体系、AV、启发式检测、流量特征检测 | | | |
| 日志查询 | 提供上网行为日志、外发内容/文件查询 | | | |
| 专项报表 | 基于流量、时长、次数，分别提供用户、应用的排行、趋势、对比报表 | | | |
| 综合报表 | 工作效率、带宽利用、威胁过滤、合规性等多种评估分析报表 | | | |
| 日志存储 | 支持内置和外置两种方式，存储审计日志数据 | | | |
| 攻击防范 | 防范多种DoS和DDoS、扫描窥探、畸形报文等攻击 | | | |
| 高可靠性 | HA（含网关模式VRRP、设备异常时平滑切换）、冗余电源（2600/2800）、硬件Bypass | | | |
| **物理特性** | | | | |
| 尺寸（W*D*H）mm | 442x420X43.6mm | | 442×560×43.6mm | |
| 重量 | 8kg | | 9kg | |
| 电源规格 | 100W AC：100～240V 50/60Hz | | 150W AC：100～240V 50/60Hz | |
| 工作环境 | 温度：0~40℃<br>湿度：10%～90%　不结露 | | 温度：0~40℃<br>湿度：5%～95%　不结露 | |
| MTBF | 12.67年 | | 16.67年 | |